the compromise of vital national defense plans or cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(2) *Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of ''serious damage'' include, but are not limited to, disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

(3) *Confidential* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

(c) Classification restraints. (1) The classification level of any form of information is premised on an evaluation of its contents as a whole, as well as on its relationship to other information.

(2) In classifying information, the public's interest in access to government information must be balanced against the need to protect national security information.

(3) In case of doubt, the lower level of classification is to be used.

(d) Duration of classification. (1) Information shall be classified for as long as is required by national security considerations, subject to the limitations set forth in section 1.6 of the Executive Order. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified. If a specific date or event for declassification cannot be determined, information shall be marked for declassification 10 years from the date of the original decision, except that the original classification authority may classify for a period greater than 10 years specific information that falls within the criteria set forth in section 1.6(d) of the Executive Order.

(2) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time except for records that are more than 25 years old.

(3) Information classified for an indefinite duration under predecessor orders, such as ''Originating Agency's Determination Required,'' shall be subject to the declassification provisions of Part 3 of the Executive Order, including the provisions of section 3.4 regarding automatic declassification of records older than 25 years.

§605.5 Classification authority.

(a) *General.* Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization, or agency.

(b) *Designations.* The following ACDA officials shall have original classification authority in each of the three designations under which they are shown below. This authority vests only in the officials or positions designated and, except as provided in paragraph (c) of this section, may not be redelegated. In the absence of any of the authorized classifiers (for TDY outside Washington, annual leave, temporary position vacancy, etc.), the officer acting in that person's position may exercise the classifier's authority.

(1) *Top Secret.* (i) Director,

(ii) Deputy Director.

(2) *Secret.* (i) Officials having Top Secret classification authority,

(ii) such other officials who have a frequent need to exercise Secret authority and are specifically delegated this authority in writing by the Director.

(3) *Confidential.* (i) Officials having Top Secret and Secret classification authority,

(ii) Other officials who have a frequent need to exercise Confidential authority and are specifically delegated this authority in writing by the Director.

(c) Delegation of classification authority. (1) The Executive Order restricts delegation of original classification authority to officials who have a demonstrable and continuing need to exercise such authority. Such delegations shall be held to a minimum.

(2) If in the judgment of bureau or office heads an officer has a demonstrable need for classification authority, a written request over the bureau or office head's signature should be forwarded via the Director of Security to the Deputy Director for action. The request should set forth the officer's name and title, the justification for having the authority, and the level of classification authority sought.

(3) The Director of Security shall maintain a complete current list by classification designation of individuals to whom and positions to which original classification authority has been delegated.

(4) Periodic reviews of delegations of classification authority will be made by the Director of Security to ensure that officials so designated have a continuing need to exercise such authority. Recommendations by the Director of Security for discontinuance of delegations will be forwarded to the Deputy Director for action.

(5) Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classifications markings derived from source material or as directed by a classification guide.

(d) Classification responsibilities. Each ACDA officer who signs, authenticates, or otherwise produces a document is responsible for determining that it is properly classified and marked. This responsibility includes determining whether the document contains any originally classified material (in which case the classification must be authorized by an appropriate ACDA classifying official) or contains information already classified (in which case the proper derivative markings must be applied). Any significant doubt about the level of classification shall be resolved in favor of the lower level.

(e) Classification challenges. Holders of information who believe that its classification status is improper are expected and encouraged to challenge the need for classification, the classification level, the duration of classification, the lack of classification or other aspect believed to be improper. Classification challenges shall be directed to and decided by the Deputy Director. If the information was not originated within or classified by ACDA, it will be referred to the Classification Adviser for coordination with the responsible agency or department if declassification, downgrading, classification or other change in its status appears to be warranted. Individuals making challenges to the classification status of information shall not be subject to retribution for such action, and they shall be advised of their right to appeal the Deputy Director's decision on the challenge to the Interagency Security Classification Appeals Panel established by section 5.4 of the Executive Order.

(f) Contractor classification authority. (1) Each ACDA contract calling for classified work shall be processed under the National Industrial Security Program.

(2) Each contract processed under the National Industrial Security Program requires the preparation of a contract security classification specification (DD 254) which serves as the contractor's guidance and authority to apply classification markings.

(3) Each contract processed under the Department of Energy (DOE) Security Requirements (i.e., involving restricted data or formerly restricted data) shall include a provision for naming a classification coordinator in the contractor organization. This individual shall coordinate the derived classification of all documents prepared under the contract in accordance with guidance received from ACDA via the ACDA Contracting Officer's Technical Representative for the contract, or by direct consultation on classification problems with the ACDA Classification Adviser or the Director of Security.

(4) Only designated officials of the U.S. Government may originally classify information. Contractor personnel, as potential developers of classified information, must follow the guidelines

outlined in paragraph (d) of this section entitled ''Classification Responsibilities.'' When there is a question involving the original classification of information, the contractor is obligated to safeguard it in accordance with the classification designation deemed appropriate and submit recommendations to ACDA for classification determination.

(5) In general, the classification of the information provided by ACDA for use or reference in the completion of the contract will be the source of the classification of documents prepared under the contract.

§605.6 Derivative classification.

(a) *Definition.* Derivative classification is the incorporating, paraphrasing, restating or generating in new form information that is already classified and the marking of the new material consistent with the classification of the source material. Duplication or reproduction of existing classified information is not derivative classification.

(b) *Responsibility.* Derivative application of classification markings is the responsibility of those who prepare material using information that is already classified and of those who apply markings in accordance with instructions from an authorized classifier or in accordance with an authorized classification guide.

(c) *Classification guides.* (1) Classification guides used to direct derivative classification and issued by ACDA shall specifically identify the information to be protected, using categorization to the extent necessary to ensure that the information involved can be identified readily and uniformly.

(2) Each classification guide issued by ACDA shall be approved by the Senior Agency Official.

(3) Each classification guide issued by ACDA shall be kept current and shall be reviewed as required by directives issued under the Executive Order. The Director of Security shall maintain a list of all classification guides.

§605.7 Declassification and downgrading.

(a) *Declassification processes.* Declassification of classified information may occur:

(1) after review of material in response to a Freedom of Information Act (FOIA), mandatory declassification review, discovery, subpoena, or other information access or declassification request;

(2) after review as part of ACDA's systematic declassification review program;

(3) as a result of the elapse of the time or the occurrence of the event specified at the time of classification;

(4) by operation of the automatic declassification provisions of section 3.4 of the Executive Order with respect to material more than 25 years old.

(b) *Downgrading.* When material classified at the Top Secret level is reviewed for declassification and it is determined that classification continues to be warranted, a determination shall be made whether downgrading to a lower level of classification is appropriate. If downgrading is determined to be warranted, the classification level of the material shall be changed to the appropriate lower level.

(c) *Authority to downgrade and declassify.* (1) Classified information may be downgraded or declassified by the official who originally classified the information if that official is still serving in the same position, by a successor in that capacity, by a supervisory official of either, by the Classification Adviser, or by any other official specifically designated by the Deputy Director. Contractor personnel do not have authority to downgrade or declassify.

(2) The Director of Security shall maintain a record of ACDA officials specifically designated by the Deputy Director as declassification authorities.

(d) *Declassification after balancing public interest.* It is presumed that information that continues to meet classification requirements requires continued protection. In exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the ACDA official with Top Secret authority having primary jurisdiction over the information in question. That official, after consultation with the